

ACG TECHNOLOGIES LTD (T/A AKORN) PRIVACY POLICY

ACG Technologies Ltd, (trading as “Akorn”, “We”, “Us”, “Our”) is committed to protecting your personal information and respecting your privacy.

SCOPE OF THIS PRIVACY POLICY

This policy applies to the use of Akorn services (“Services”) accessed through the akorn website (www.akorn.app), its mobile and web applications, and all communication made to and from akorn customer service representatives, including but not limited to communication via phone call, email, SMS, WhatsApp, and push notification. For the avoidance of doubt, this includes an application for an e-current account and debit card (together the “Platform”).

This policy sets out the basis on which any personal data We collect from you, or that you provide to Us, will be processed by Us. Please read the following carefully to understand Our views and practices regarding Our treatment of your personal data.

For the purposes of applicable data protection laws (including the Data Protection Act 2018, UK General Data Protection Regulation and the Privacy and Electronic Communication Regulations – PECR) (“Data Protection Laws”), the data controller is ACG Technologies Ltd, trading as Akorn. ACG Technologies Ltd is registered in England and Wales under company number 12902368. Our registered office is located at 24 Great Chapel Street, London, United Kingdom, W1F 8FS.

INFORMATION WE COLLECT ABOUT YOU

Akorn may collect and process the personal data of Service Users (“Users”) including:

- Information Users give Us which includes a User’s full title, full name, address(es), date of birth, passport/ID, nationality, mobile phone number, mobile device information, email address, and financial transaction information (“Submitted Information”).
- Registration and correspondence: Users may give Us information by registering for our Services via the Platform, or by corresponding with Us (for example, by e-mail). If Users contact Us, we may keep a record of that correspondence.
- Device Information: Following consent, each time Users use Services, We may collect the following information about Users and their Devices:
 - Technical Information: including the User’s type of mobile device, unique device identifier (e.g. the Device’s IMEI number, the MAC address of the Device’s wireless network interface, or the mobile phone number used by the Device), mobile network information, the User’s mobile operating system, the type of mobile browser and time zone setting (“Device Information”);

- Details of use of Services, including by not limited to traffic data and location data (“Log Information”).

PROCESSING PURPOSES OF USER DATA

Akorn collects and processes the personal data of Users for the following purposes:

- To provide Akorn Services – We collect and process User data primarily for the provision and effective use of Akorn Services. Submitted information is used by Us to provide the Services.
- To provide customer service
- To market our Platform and Services – In using the Platform and Services, Users will be asked to provide consent to the use of personal data to market Our Services. Users have the right to withdraw consent to marketing at any time by contacting Us.
- To enable third party integrations – We will only disclose User personal data to Our regulated e-money issuer (“Banking Partner”), and not to any other third party. If you wish to learn more about how our Banking Partner processes your data, you can do so by visiting: <https://www.railsr.com/privacy-policy>
- To develop our Platform and Services – We will use Device Information and Log Information for Our understanding of how Users use Services to ensure Services are optimized for your use.

LAWFUL BASES FOR PROCESSING USER DATA

We will only use your personal data when and where the law allows/compels us to.

- **Performance of contract** – When processing personal data for the purpose of providing Akorn Services, We process on the basis of a contract to which you are party or to take steps at your request before entering into such a contract. This is formed when you create your account and accept Our terms and conditions. Before We provide services to Users, We are legally required to carry out checks for the purposes of preventing fraud and money laundering/terrorist financing and to verify your identity.
- **Legitimate Interest** – We process User data where it is necessary for our legitimate interests (or those of a third party), and User interests and fundamental rights do not override those interests.
 - Legitimate interest means the interest of our business in conducting, managing, and protecting our business to enable us to give Users the best service and the best and most secure experience. One of our legitimate interests is preventing money laundering/terrorist financing, fraud, and

verifying identity. When choosing to use your data on the basis of our legitimate interests, we carefully weigh our own interests against your rights, in compliance with the law. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting Us.

- **Legal Obligation** – We must process certain information to comply with statutory obligations that We are subject to, including data you have provided, we have collected from you or received from third parties. In light of the obligation to prevent fraud, money laundering, and terrorist financing, and, with the help of our Banking Partner and fraud prevention agencies, we may enable law enforcement agencies to access and use your personal data to detect, investigate and prevent crime.
 - If we, or a fraud prevention agency, determine that a User poses a fraud or money laundering/terrorist financing risk, we may refuse to provide existing or requested Services. A record of any fraud and money laundering/terrorist financing risk will be retained by fraud preventing agencies and may result in others refusing to provide services and financing to you. If you have any further questions about this, please contact us at help@akorn.app.
- **Consent** – Generally, We do not rely on consent as a legal basis for processing your personal data, except where we are processing special categories of data such as biometric data contained in a passport when we will require your explicit consent. We will get your consent before sending direct marketing communications to you via email or text message (subject to the right to withdraw consent).
- **Automated Decision Making** – As part of Our processing of your personal data, decisions may be made by automated means. This means that We, or our data processors, may automatically decide a User poses a fraud or money laundering/terrorist financing risk if Our processing reveals your behaviour to be consistent with money laundering/terrorist financing or known fraudulent conduct, is inconsistent with other data held, or appears to be deliberately hiding true identity. Users have rights in relation to automated decision making. If you want to know more, please contact us at help@akorn.app.

DISCLOSURE OF YOUR INFORMATION

We will only disclose your personal data to Our regulated e-money issuer (“Banking Partner”), and not to any other third party.

STORAGE OF PERSONAL DATA

The data that We collect from you will be stored within the UK and EEA. By submitting your personal data, you agree to this transfer, storing and/or processing. We will take all steps reasonably necessary to ensure that your data is treated securely and with the appropriate technical and organisational measures in accordance with this privacy policy.

Where We have given you (or where you have chosen) a password that enables you to access the Services, you are responsible for keeping this password confidential. We ask you not to share a password with anyone.

Unfortunately, the transmission of information via the Internet is not completely secure. Although We will do Our best to protect your personal data, We cannot guarantee the security of your data when it is transmitted; any transmission occurs at your own risk. Once We have received your information, We will use strict procedures and security features to prevent unauthorised access.

DATA RETENTION

We will only retain your personal data for as long as reasonably necessary to fulfil the purposes We collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal data for a longer period in the event of a complaint or if We reasonably believe there is a prospect of litigation in respect to Our relationship with you.

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which We process your personal data and whether We can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

By law We have to keep basic information about our customers (including Contact, Identity, and Financial Data) for six years for regulatory purposes. Please note that fraud prevention agencies are permitted to hold your personal data for different periods of time and if you are considered to pose a fraud or money laundering/terrorist financing risk your data can be held for up to six years.

USE OF COOKIES

We may collect and store personal data on your device using application data caches and browser web storage and other technology.

Please see our Cookie Policy for more information on Akorn's use of cookies.

YOUR RIGHTS AS A DATA SUBJECT

Whenever Akorn processes your data, you have certain rights, in accordance with applicable Data Protection Laws, including the right to access your personal data, the right to rectification, a right to restrict Our processing activities of your data, the right to data portability, and a right of erasure.

Right to access data

The applicable Data Protection Laws give you the right to access information held about you. Your right of access can be exercised in accordance with such Data Protection Laws. You

will not have to pay a fee to access your personal data (or exercise any of the other rights). However, We may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, We could refuse to comply with your request in these circumstances.

Right to object to processing

You have the right to object to the processing of your personal data for any marketing purposes. You will be required to provide your consent to the processing of your Submitted Information by checking certain boxes on the Platform and other systems controlled by Akorn. You have the right to withdraw your consent at any time. You can contact Us at help@akorn.app for further information.

The Platform and Services may, from time to time, contain links to and from the websites of Our partner networks, third-party employers, advertisers, and affiliates. If You follow a link to any of these websites, please note that these websites and any services that may be accessible through them have their own privacy policies and that We do not accept any responsibility or liability for these policies or for any personal data that may be collected through these websites or services, such as contact and location data. Please check these policies before you submit any personal data to these websites or use these services.

CHANGES TO THIS PRIVACY POLICY

We reserve the right to update this Policy from time to time at our sole discretion. Any changes We may make to Our Privacy Policy in the future will be posted on this page and, where appropriate, notified to you by e-mail or when you next start the Services including where We are required to obtain either revised or additional consent from you with regards to the collection, transfer and processing of your personal data. The new terms may be displayed on-screen and you may be required to read and accept them to continue your use of the Services. If you keep using Akorn Services after a change, your continued use means that you accept any such changes.

CONTACT INFORMATION

Questions, comments, and requests regarding this privacy policy are welcomed and should be addressed to help@akorn.app

Last updated 30 November 2022